

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

LINDA BOOTH, MARY NAPIER, and
CANDACE DAUGHERTY on behalf of
themselves and all others similarly situated,

Plaintiffs,

vs.

MCG Health, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Linda Booth, Mary Napier, and Candace Daugherty, individually and on behalf of the proposed class defined below, bring this action against Defendant MCG Health, LLC (“MCG”) allege as follows:

I. SUMMARY OF THE ACTION

1. This action arises out of MCG’s failure to secure the highly sensitive personal information of its patients. Around February 25 to 26, 2020, an unauthorized party or parties accessed MCG’s computer systems and exfiltrated patient files (the “Data Breach”). MCG did not learn of the breach until more than two years later, on March 25, 2022 and determined that the exfiltrated files contained patient names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and genders. Over 1,100,000 patients’ personally identifiable information (“PII”) and personal health information (“PHI”) was compromised in the attack.

2. Even after MCG learned of the hack on March 25, 2022, it did not notify affected patients of the attack until June 10, 2022. During this time, those patients remained unaware that

1 their information had been compromised. The personal information remains in the possession of the
 2 unauthorized party or parties.

3 3. As a result of MCG's data security failures, Plaintiffs and Class members confront a
 4 significant threat of identity theft and other harm—imminently and for years to come. Plaintiffs by
 5 this action seek damages together with injunctive relief to remediate MCG's deficient cybersecurity
 6 protocols and provide identity theft insurance (or the money needed to secure those services) to
 7 protect them and the other breach victims from identity theft and fraud.

8 II. PARTIES

9 *Plaintiff Linda Booth*

10 4. Plaintiff Linda Booth is a citizen and resident of Santa Fe, New Mexico.

11 5. Plaintiff Booth received a letter dated June 10, 2022 from MCG notifying her of the
 12 Data Breach and stating that it "affects certain of your personal information." The letter stated that an
 13 unauthorized party "previously obtained certain of your personal information that matched data stored
 14 on MCG's systems." Affected information includes names, Social Security numbers, medical codes,
 15 postal addresses, telephone numbers, email addresses, dates of birth, and gender.

16 *Plaintiff Mary Napier*

17 6. Plaintiff Mary Napier is a citizen and resident of Rogers, Kentucky

18 7. Plaintiff Napier received a letter dated June 10, 2022, from MCG notifying her of the
 19 Data Breach and stating that it "affects certain of your personal information." The letter stated that an
 20 unauthorized party "previously obtained certain of your personal information that matched data stored
 21 on MCG's systems." Affected information includes names, Social Security numbers, medical codes,
 22 postal addresses, telephone numbers, email addresses, dates of birth, and gender.

23 *Plaintiff Candace Daugherty*

24 8. Plaintiff Candace Daugherty is a citizen and resident of Vancleave, Mississippi.

25 9. Plaintiff Daugherty received a letter dated June 10, 2022, from MCG notifying her of
 26 the Data Breach and stating that it "affects certain of your personal information." The letter stated that
 27 an unauthorized party "previously obtained certain of your personal information that matched data

1 stored on MCG's systems." Affected information includes names, Social Security numbers, medical
 2 codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender.

3 10. Defendant MCG Health, LLC is a Washington limited liability corporation with its
 4 principal place of business in Seattle, Washington.

5 **III. JURISDICTION AND VENUE**

6 11. This Court has jurisdiction over the lawsuit under the Class Action Fairness Act, 28
 7 U.S.C. § 1332, because this is a proposed class action in which: (1) there are at least 100 class
 8 members; (2) the combined claims of Class members exceeds \$5,000,000, exclusive of interest,
 9 attorneys' fees, and costs; and (3) MCG Health and Class members are domiciled in different states.

10 12. This Court has personal jurisdiction over Defendant MCG health because its
 11 principal place of business is within this District, and it has sufficient minimum contacts in
 12 Washington to render the exercise of jurisdiction by this Court proper and necessary.

13 13. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part
 14 of the events or omissions giving rise to the claims occurred in this District.

15 **IV. FACTUAL ALLEGATIONS**

16 **MCG Health and the Data Breach**

17 14. MCG is a HIPPA business associate that provides care guidelines to healthcare
 18 providers and health plans. A HIPPA business associate is an entity that provides services to a
 19 HIPPA covered entity (i.e., a hospital) that involves the disclosure of personal health information.
 20 HIPPA business associates are often software companies that have access to large quantities of
 21 personal health information.

22 15. MCG develops and institutes software and evidence-based care guidelines to assist
 23 healthcare payers, providers, and government healthcare agencies in making decisions related to
 24 patient care.

25 16. MCG Health is part of the Hearst Health network. MCG states that a "majority of
 26 U.S. health plans and nearly 2,600 hospitals" use their services.

1 17. For the past 30 years, MCG has worked with state, regional, and federal government
2 healthcare agencies and government contractors, in government administered healthcare programs.

3 18. As part of its business operations, MCG collects from Plaintiffs and Class Members
4 or the healthcare networks, providers, and plans that they use, information including names, Social
5 Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of
6 birth, and genders.

7 19. On March 25, 2022, MCG discovered that an unauthorized party accessed patient
8 and member data stored on MCG's systems. MCG states that "there is evidence to suggest the data
9 may have been acquired by an unauthorized party on or around February 25-26, 2020." MCG,
10 however, also asserts that it is uncertain as to when the data was first acquired by unauthorized
11 parties.

12 20. Around June 10, 2022, over two years after the hack occurred and almost three
13 months after discovering the breach, MCG informed its patients and members of the data breach
14 and advised them to take protective measures. The letter stated that MCG experienced suspicious
15 activity on its computer network and an unauthorized party or parties obtained personal information
16 that matched data stored in MCG's systems. The letter informed victims of the breach that the
17 following information had been compromised: names, Social Security numbers, medical codes,
18 postal addresses, telephone numbers, email addresses, dates of birth, and gender.

19 21. Plaintiffs suffer stress and anxiety as a result of the Data Breach and from the loss of
20 their privacy.

21 22. Plaintiffs also suffered injury in the form of damage to and diminution in the value
22 of their confidential personal information—a form of property that Plaintiffs entrusted to Defendant,
23 and which was compromised as a result of the Data Breach it failed to prevent.

24 23. Plaintiffs suffer a present injury from the existing and continuing risk of fraud,
25 identity theft, and misuse resulting from their personal information being placed in the hands of
26 unauthorized third parties.

27

24. Plaintiffs have a continuing interest in ensuring that their personal information is protected and safeguarded from future breaches.

Personally Identifiable Information Has Concrete Financial Value

25. The private health information and personally identifiable information taken from MCG's system is particularly sensitive. Medical and personally identifiable information is valuable to cybercriminals and has routinely been sold and traded on the dark web.

26. PII and PHI are inherently valuable and the frequent target of hackers. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018. Of the 1,473 recorded data breaches, 525 of them, or 35.64% were in the medical or healthcare industry. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.

27. Identity theft results in a significant negative financial impact on victims as well as severe distress.

28. MCG is aware that the PII and PHI it collects is highly sensitive and of substantial value to those who would use it for wrongful purposes.

29. PII and PHI is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud. There is a robust black market in which criminals openly post stolen PII and PHI on multiple underground internet websites, commonly referred to as the dark web.

30. There is accordingly a market for Plaintiffs' and Class members' PII and PHI.

31. Sensitive healthcare data can sell for as much as \$363 per record, according to the Infosec Institute.

32. MCG states that medical codes were disclosed within the breach. Medical codes are used to convert diagnoses, procedures, medical services, and equipment into universal medical alphanumeric codes.

33. PHI, like medical codes, is particularly valuable because criminals can use it to target victims with fraud and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

34. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, misdiagnosis or mistreatment can ensue. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."¹

35. Similarly, Social Security numbers are valuable to criminals. This information can be and has been sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

36. The detrimental consequences of MCG's failure to keep its patients' and members' PII and PHI secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

37. Criminals often trade stolen PII and PHI on the "cyber black market" for years following a breach. Cybercriminals also can post stolen PII and PHI on the internet, thereby making the information publicly available without the knowledge or consent of the victim.

38. MCG knew the importance of safeguarding the PII and PHI entrusted to it and the foreseeable adverse effects if its data security systems were breached. Those effects include the

¹ Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), <https://khn.org/news/rise-of-identity-theft/> (last visited Dec. 8, 2021).

significant costs that would be imposed on affected patients as a result of a breach. MCG failed to implement adequate cybersecurity measures, leading to the Data Breach.

V. CLASS ACTION ALLEGATIONS

39. Plaintiffs bring this lawsuit as a class action on behalf of themselves and on behalf of all other persons similarly situated, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(2), (b)(3), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements.

40. The proposed Class is defined as: All United States citizens whose personally identifiable information was in MCG's electronic information systems and was compromised as a result of the Data Breach discovered by MCG on March 25, 2022.

41. Plaintiffs reserve the right to modify, change, or expand the Class definition, including by proposing subclasses, based on discovery and further investigation.

42. Excluded from the Class is the Defendant, and its officers, directors, and managerial employees. Also excluded are individuals employed by counsel for the parties in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

43. Numerosity. While the exact number of Class members is not known at this time, the Class is so numerous that joinder of all members is impractical. Over 1.1 million individuals' personal information was compromised in this attack. The identities of Class members are available through information and records in the possession, custody, or control of Defendant, and notice of this action can be readily provided to the Class.

44. Typicality. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all Class members, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions of the Defendant described herein. Plaintiffs' claims thus arise from the same course of conduct that gives rise to the claims of all Class members.

45. Adequacy of Representation. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect the other members' interests. Plaintiffs' counsel are

competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interests adverse to the interests of other Class members.

46. Predominant Common Issues of Law and Fact. There is a well-defined community of interest in the common questions of law and fact that underlie Class members' claims for relief. The questions of law and fact in this case that are common to Class members predominate over questions affecting only individual Class members. Among the questions of law and fact common to the Class are:

a. Whether the Defendant had a duty to implement reasonable cybersecurity measures to protect Plaintiffs' and Class members' sensitive personal information and to promptly alert them if such information was compromised;

b. Whether the Defendant breached its duties by failing to take reasonable precautions to protect Plaintiffs' and Class members' sensitive personal information;

c. Whether the Defendant acted negligently by failing to implement reasonable data security practices and procedures;

d. Whether the Defendant violated the Washington Consumer Protection Act, RCW 19.86, *et seq.*; and

e. Whether Plaintiffs and Class members are entitled to damages, and/or injunctive and other relief in equity.

47. Superiority. This class action is superior to other alternatives for the fair and efficient adjudication of this controversy. Absent a class action, most members of the Class would find the cost of litigating their claims individually to be prohibitively high and would have no effective remedy. Class treatment will conserve judicial resources, avoid waste and the risk of inconsistent rulings, and promote efficient adjudication before a single judge.

48. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making appropriate injunctive and declaratory relief with respect to the Class as a whole.

1 **VI. FIRST CAUSE OF ACTION**

2 **Violation of the Washington Consumer Protection Act, RCW 19.86, *et seq.***

3 49. Plaintiffs incorporate and reallege the foregoing allegations of fact.

4 50. Defendant is a “person” within the meaning of the Washington Consumer Protection
5 Act, RCW 19.86.010 and it conducts “trade” and “commerce” within the meaning of RCW
6 19.86.010(2).

7 51. Plaintiffs and Class members are “persons” within the meaning of RCW
8 19.86.010(1).

9 52. Defendant engaged in unfair or deceptive acts or practices in the conduct of its
10 business by the conduct set forth above. These unfair or deceptive acts or practices include the
11 following:

12 a. Failing to adequately secure Plaintiffs’ and Class members’ personal
13 information from disclosure to unauthorized third parties or for improper purposes;

14 b. Enabling the disclosure of personal and sensitive facts about Plaintiffs and
15 the Class in a manner highly offensive to the reasonable person;

16 c. Enabling the disclosure of personal and sensitive facts about Plaintiffs and
17 the Class without their informed, voluntary, affirmative, and clear consent;

18 d. Omitting, suppressing, and concealing the material fact that Defendant did
19 not reasonably or adequately secure Plaintiffs’ and Class members’ personal information; and

20 e. Failing to disclose the data breach in a timely and accurate manner.

21 53. Defendant’s systematic acts or practices are unfair because the acts or practices are
22 immoral, unethical, oppressive, and/or unscrupulous.

23 54. Defendant’s systematic acts or practices are deceptive because they were and are
24 capable of deceiving a substantial portion of the public.

25 55. Defendant’s unfair or deceptive acts or practices have repeatedly occurred in trade of
26 commerce within the meaning of RCW 19.86.010 and RCW 19.86.020.

1 taking other reasonable security measures to safeguard and adequately secure the personal
2 information of Plaintiffs and the Class from unauthorized access and use.

3 65. Defendant owed a duty of care to Plaintiffs and Class members to establish cyber
4 security measures consistent with the standards of care from statutory authority like HIPPA.

5 66. HIPPA requires that a covered entity, like MCG, “must have in place appropriate
6 administrative, technical, and physical safeguards to protect the privacy of protected health
7 information.” 45 C.F.R. § 164.530. Information exposed in the data breach constitutes as “protected
8 health information.”

9 67. Plaintiffs and Class members were the foreseeable victims of Defendant’s
10 inadequate cybersecurity. The natural and probable consequence of Defendant’s failing to
11 adequately secure their information networks was Plaintiffs’ and Class members’ personal
12 information being hacked.

13 68. Defendant knew or should have known that Plaintiffs’ and Class members’ personal
14 information was an attractive target for cyber thieves, particularly in light of data breaches affecting
15 other medical and non-medical entities. The harm to Plaintiffs and Class members from exposure of
16 their extremely confidential personal information was reasonably foreseeable to Defendant.

17 69. Defendant had the ability to sufficiently guard against data breaches by
18 implementing adequate measures to protect its networks, such as by ensuring best practices in
19 cybersecurity defense, enhancing its security measures, and increasing network monitoring.

20 70. Defendant breached its duty to exercise reasonable care in protecting Plaintiffs’ and
21 Class members’ personal information by failing to implement and maintain adequate security
22 measures to safeguard Plaintiffs’ and Class members’ personal information, failing to monitor its
23 systems to identify suspicious activity, and allowing unauthorized access to, and exfiltration of,
24 Plaintiffs’ and Class members’ highly confidential personal information.

25 71. Defendant’s duties also arise by operation of statute. The Washington Data Breach
26 Notice Act, RCW 19.255, *et seq.*, requires that MCG also owed a duty to timely disclose to
27 Plaintiffs and Class members that their personal information had been or was reasonably believed to

1 have been compromised. Timely disclosure was necessary so that Plaintiffs and Class members
2 could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2)
3 monitor their credit reports, financial accounts, and other records; and (3) take other steps to protect
4 themselves and attempt to avoid or recover from identity theft.

5 72. Defendant breached its duty to timely disclose the Data Breach to Plaintiffs and
6 Class members. Defendant did not learn of the Data Breach until over two years after the hack
7 occurred. And even after learning of the Data Breach, Defendant unreasonably delayed in notifying
8 Plaintiffs and Class members of the Data Breach. This unreasonable delay caused foreseeable harm
9 to Plaintiffs and Class members by preventing them from taking timely self- protection measures in
10 response to the Data Breach.

11 73. There is a close connection between Defendant's failure to employ reasonable
12 security protections for its patients' and members' personal information and the injuries suffered by
13 Plaintiffs and Class members. When individuals' extremely sensitive personal information is stolen,
14 they face a heightened risk of identity theft and may need to: (1) purchase identity protection,
15 monitoring, and recovery services; (2) monitor their credit reports, financial accounts, and other
16 records; and (3) take other steps to protect themselves and attempt to avoid or recover from identity
17 theft.

18 74. The policy of preventing future harm disfavors application of the economic loss rule,
19 particularly given the extreme sensitivity of the private information entrusted to Defendant. A high
20 degree of opprobrium attaches to Defendant's failure to secure Plaintiffs' and Class members'
21 personal and extremely confidential details. Defendant had an independent duty in tort to protect
22 this information and thereby avoid reasonably foreseeable harm to Plaintiffs and Class members.

23 75. As a result of Defendant's negligence, Plaintiffs and Class members have suffered
24 damages that have included or may, in the future, include, without limitation: (1) loss of the
25 opportunity to control how their personal information is used; (2) diminution in the value and use of
26 their personal information entrusted to Defendant with the understanding that Defendant would
27 safeguard it against theft and not allow it to be accessed and misused by unauthorized third parties;

(3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft; (5) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

76. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

77. Plaintiffs and Class members are therefore entitled to an award of damages against Defendant and injunctive relief in the form of an order prohibiting Defendant from engaging in the alleged misconduct.

VIII. THIRD CAUSE OF ACTION

Invasion of Privacy

78. Plaintiffs incorporate and reallege the foregoing allegations of fact.

79. Plaintiffs and Class members reasonably expected that the personal information they entrusted to Defendant, such as their names, Social Security numbers, addresses, and dates of birth, would be kept private and secure, and would not be disclosed to any unauthorized third party or for any improper purpose.

80. Defendant unlawfully invaded Plaintiffs' and Class members' privacy rights by:

- a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and
- c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

81. A reasonable person would find it highly offensive that Defendant, having received, collected, and stored Plaintiffs' and Class members' full names, dates of birth, and Social Security numbers and other highly sensitive personal details, failed to protect that information from unauthorized disclosure to third parties.

82. In failing to adequately protect Plaintiffs' and Class members' personal information, Defendant acted knowingly and in reckless disregard of their privacy rights. Defendant knew of the recent security breaches experienced by other medical and healthcare providers. Defendant also knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiffs' positions.

83. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

84. Defendant's unlawful invasions of privacy damaged Plaintiffs and Class members. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs and Class members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated. Accordingly, Plaintiffs and Class members are entitled to damages in an amount to be determined at trial.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for an Order:

- A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel to represent the Class;
- B. Entering judgment for Plaintiffs and the Class;
- C. Awarding Plaintiffs and Class members monetary relief;
- D. Ordering appropriate injunctive or other equitable relief;
- E. Awarding pre- and post-judgment interest as prescribed by law;
- F. Awarding reasonable attorneys' fees and costs as permitted by law; and
- G. Granting such further and other relief as may be just and proper.

X. REQUEST FOR JURY TRIAL

Plaintiffs seek a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 22nd day of June, 2022.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759

By: /s/ Jennifer Rust Murray, WSBA #36983

Jennifer Rust Murray, WSBA #36983

936 North 34th Street, Suite 300

Seattle, Washington 98103-8869

Telephone: (206) 816-6603

Facsimile: (206) 319-5450

Email: bterrell@terrellmarshall.com

Email: jmurray@terrellmarshall.com

Adam E. Polk, *Pro Hac Vice Forthcoming*

Simon Grille, *Pro Hac Vice Forthcoming*

Jessica Cook, *Pro Hac Vice Forthcoming*

GIRARD SHARP LLP

601 California Street, Suite 1400

San Francisco, California 94108

Telephone: (415) 981-4800

Facsimile: (415) 981-4846

Email: apolk@girardsharp.com

Email: sgrille@girardsharp.com

Email: jcook@girardsharp.com

Attorneys for Plaintiffs